

# RECUEIL DES POLITIQUES ET PROCÉDURES DU CHUQ

<b>OBJET :</b> POLITIQUE EN MATIÈRE DE SÉCURITÉ INFORMATIONNELLE	<b>POLITIQUE N°</b> 02-7100
<b>DESTINATAIRES :</b> Tous les utilisateurs des systèmes d'information du CHUQ	<b>Date d'approbation :</b> 2010-09-27
<b>ÉMISE PAR :</b> Direction des technologies de l'information	<b>Date d'entrée en vigueur :</b> 2010-09-27
<b>APPROUVÉE PAR :</b> Le conseil d'administration <i>Original signé par Gertrude Bourdon, secrétaire</i>	<b>Date de la dernière révision (modification) :</b>

## 1. OBJET

La Politique en matière de sécurité informationnelle (*Politique*) vise à établir les règles du Centre hospitalier universitaire de Québec (CHUQ) en mettant en place, tant sur support papier qu'électronique, un ensemble de mesures de sécurité et de contrôle afin de protéger les renseignements personnels informatisés.

L'établissement se doit de gérer adéquatement l'utilisation d'Internet, du courrier électronique et des réseaux d'information du CHUQ, et ce, autant en ce qui concerne la recherche scientifique, l'enseignement, le domaine médico-administratif ou tout autre mandat qui pourrait lui être confié. Ceci ne restreint pas la mise en place de mesures de sécurité supplémentaires ou plus restrictives visant à assurer la protection des documents personnels qui sont confiés à chaque organisme ou établissement du CHUQ ou en faisant partie.

## 2. CADRE JURIDIQUE ET ADMINISTRATIF

Les principes directeurs qui sous-tendent cette *Politique* sont tirés du [Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – Volet sur la sécurité](#), approuvé par le ministère de la Santé et des Services sociaux le 24 septembre 2002.

Ce document précise les orientations et les obligations que doivent respecter les organismes du réseau de la santé et des services sociaux en matière de sécurité de l'information. Ces principes concernent la cueillette, la confidentialité des renseignements personnels et leur communication, l'accès aux données confidentielles, aux actifs informationnels et de télécommunication et à l'ensemble des activités relatives à l'acquisition, à la production, au traitement, à l'entreposage, au transfert et à l'impression, ainsi qu'à la disposition des informations.

Cette *Politique* doit mettre en place des mesures et des mécanismes administratifs et de contrôle afin d'assurer le respect des droits des usagers, tel que stipulé dans la :

- [Charte des droits et libertés de la personne](#);
- [Loi concernant le cadre juridique des technologies de l'information](#);
- [Loi sur les services de santé et les services sociaux](#);
- [Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels \(Loi sur l'accès\)](#).

<b>RENOI(S) :</b> Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)
--

<b>OBJET :</b> POLITIQUE EN MATIÈRE DE SÉCURITÉ INFORMATIONNELLE	<b>POLITIQUE N° 02-7100</b>
---	-----------------------------

### 3. CHAMP D'APPLICATION

La *Politique* s'applique à tous les utilisateurs des systèmes d'information qui, de près ou de loin, peuvent avoir accès aux actifs informationnels et de télécommunication ainsi qu'aux documents qu'ils supportent, dont notamment les bénévoles, chercheurs, dentistes, médecins, stagiaires, fournisseurs, ainsi que le personnel du CHUQ.

La *Politique* s'applique :

- À tous les actifs informationnels et de télécommunication appartenant au CHUQ ou sous sa responsabilité;
- Aux contrats ou aux ententes de service avec tout intervenant externe; les ententes doivent contenir les dispositions requises pour garantir le respect de la *Politique* et des règles qui en découlent.

Cette *Politique* couvre, de même, tous les documents traités par le CHUQ dans le cadre de ses fonctions et de ses mandats. Par conséquent, tout le matériel informatique qui conserve, transmet et traite des données informatiques, quel que soit le type de support utilisé (bandes magnétiques, disquettes, CD-ROM, clés USB, listes ou toute autre forme) est assujéti à la *Politique*, de même que toute la gestion et la disposition des documents et des informations qu'ils contiennent.

#### 3.1. ENGAGEMENT DE CONFIDENTIALITÉ PAR L'UTILISATEUR

Tous les utilisateurs doivent signer un engagement de confidentialité avec le CHUQ (cf. [Annexe 1](#)).

### 4. DÉFINITIONS

#### 4.1. ACTIFS INFORMATIONNELS ET DE TÉLÉCOMMUNICATION

Banque d'information électronique, système d'information, réseau de télécommunication, technologies de l'information, installation ou ensemble de ces éléments; un équipement médical spécialisé ou ultraspécialisé peut comporter des composantes qui font partie des actifs informationnels, notamment lorsqu'il est relié de façon électronique à des actifs informationnels; s'ajoutent dans le présent document les documents imprimés par les technologies de l'information.

#### 4.2. AUDIT

Évaluation périodique basée sur des critères définis permettant de vérifier si les normes en vigueur sont appliquées.

#### 4.3. AUTHENTIFICATION

Fonction de contrôle de l'accès aux actifs informationnels permettant d'établir la validité de l'identité d'un utilisateur, d'un dispositif ou d'une autre entité au sein d'un système d'information ou de communications.

<b>RENOI(S) :</b> Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)	Page 2 de 15  DIC : 1-2-1
---	---------------------------------

**OBJET :** POLITIQUE EN MATIÈRE DE SÉCURITÉ  
INFORMATIONNELLE

**POLITIQUE N° 02-7100**

#### 4.4. CONFIDENTIALITÉ

Propriété que possède une donnée ou une information dont l'accès et l'utilisation sont réservés à des personnes ou entités désignées et autorisées, conformément à la *Politique* et aux documents qui s'y rapportent ainsi qu'aux lois pertinentes en vigueur au Québec.

#### 4.5. DISPONIBILITÉ

Propriété qu'ont les données, l'information et les systèmes d'information et de communication d'être accessibles et utilisables en temps voulu et de la manière adéquate par une personne autorisée.

#### 4.6. ENGAGEMENT DE CONFIDENTIALITÉ

Entente écrite par laquelle l'utilisateur s'engage à respecter la *Politique relative à la confidentialité* et les codes de conduite qui en découlent.

#### 4.7. GESTIONNAIRE DE SYSTÈME

Tout membre du personnel dont la fonction est d'assurer la responsabilité de gestion d'actifs informationnels, d'équipements, de systèmes ou de réseaux au sens de la *Politique* et toute personne à qui cette responsabilité est conférée en vertu d'une entente avec le CHUQ.

#### 4.8. INTÉGRITÉ

Propriété d'une information ou d'une technologie de n'être ni modifiée, ni altérée, ni détruite d'une façon erronée ou non autorisée.

#### 4.9. INTRANET

Réseau de télécommunication privé, destiné à l'usage exclusif d'un organisme, qui utilise les mêmes protocoles et technologies que le réseau Internet.

#### 4.10. POLITIQUE

Énoncé officiel de principes généraux indiquant la ligne de conduite que les membres d'un organisme doivent observer; c'est une orientation générale, stratégique ou organisationnelle qui découle de grands principes directeurs.

#### 4.11. PRIVILÈGES D'ACCÈS

Autorisation accordée par le supérieur immédiat à un utilisateur définissant l'usage qu'il peut faire des actifs informationnels et de télécommunication.

#### 4.12. RENSEIGNEMENTS PERSONNELS

Données qui concernent une personne physique et qui permettent de l'identifier.

#### 4.13. RITM

Réseau intégré de télécommunication multimédia, anciennement désigné Réseau de télécommunications sociosanitaires « RTSS<sup>MO</sup> ».

#### RENVOI(S) :

Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2)  
Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)

Page 3 de 15

DIC : 1-2-1

<b>OBJET :</b> POLITIQUE EN MATIÈRE DE SÉCURITÉ INFORMATIONNELLE	<b>POLITIQUE N° 02-7100</b>
---	-----------------------------

## 5. PRINCIPES DIRECTEURS

Le Centre hospitalier universitaire de Québec reconnaît :

- Que nul ne peut, au nom d'un organisme public, recueillir un renseignement personnel si cela n'est pas nécessaire à l'exercice des attributions de cet organisme ou à la mise en œuvre d'un programme dont il a la gestion. Sous réserve des modalités prévues à la *Loi sur l'accès*, un organisme public peut toutefois recueillir un renseignement personnel si cela est nécessaire à l'exercice des attributions ou à la mise en œuvre d'un programme de l'organisme public avec lequel il collabore pour la prestation de services ou pour la réalisation d'une mission commune;
- Que le dossier d'un usager est confidentiel et nul ne peut y avoir accès, si ce n'est avec le consentement de l'usager ou de la personne pouvant donner un consentement en son nom. Un renseignement contenu au dossier d'un usager peut toutefois être communiqué sans son consentement dans les cas où le tribunal ou le coroner l'ordonne ou lorsqu'une loi le prévoit expressément. À cet égard, nous référons le lecteur à l'article 19 de la [Loi sur les services de santé et les services sociaux](#) quant à une liste non exhaustive des principales exceptions au principe du consentement;
- Que l'accès aux actifs informationnels et de télécommunication du CHUQ par l'utilisateur doit être contrôlé. Le CHUQ limite l'accès à ses actifs informationnels et de télécommunication aux seuls utilisateurs dont les tâches l'exigent dans l'exercice normal de leurs fonctions et qui détiennent en conséquence un privilège d'accès approprié;
- Qu'Internet, l'intranet et les réseaux d'information du CHUQ sont des outils mis à la disposition de l'utilisateur du CHUQ pour une utilisation professionnelle, plus spécifiquement pour des tâches reliées à l'exercice des fonctions de celui-ci;
- Que l'utilisateur a accès au RITM et aux réseaux d'information du CHUQ, puisque ceux-ci doivent être utilisés uniquement pour des raisons professionnelles. La *Politique en matière de sécurité informationnelle* présente des mesures de sécurité qui sont associées à l'utilisation desdits réseaux par l'utilisateur pour assurer la disponibilité, l'intégrité et la confidentialité de l'information, ainsi que l'irrévocabilité des actes posés par l'utilisateur;
- Que les messages et fichiers électroniques circulant au CHUQ sont soumis aux dispositions de la Loi<sup>1</sup>.

## 6. OBJECTIFS

La présente *Politique* a pour objectif d'assurer :

- La catégorisation des actifs informationnels, soit la disponibilité, l'intégrité et la confidentialité des documents traités par les réseaux d'information du CHUQ, communément appelée le DIC;
- La protection des renseignements personnels relatifs aux usagers par des mesures de contrôle des accès autorisés selon la législation ou l'exercice des fonctions de chaque utilisateur;

<sup>1</sup> *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et *Loi sur la protection des renseignements personnels dans le secteur privé*.

<b>RENOI(S) :</b> Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)	Page 4 de 15  DIC : 1-2-1
---	---------------------------------

<b>OBJET :</b> POLITIQUE EN MATIÈRE DE SÉCURITÉ INFORMATIONNELLE	<b>POLITIQUE N° 02-7100</b>
---	-----------------------------

- La sécurité relative à l'utilisation des réseaux d'information du CHUQ, des actifs informationnels et de télécommunication, du matériel informatique et des données personnelles;
- Le respect des différentes procédures concernant l'utilisation et la gestion des technologies de l'information et de télécommunication adoptées par le CHUQ;
- La conformité aux lois et règlements applicables ainsi qu'aux directives, normes et orientations gouvernementales.

## 7. ÉNONCÉ DE POLITIQUE

### 7.1. PRINCIPES DE SÉCURITÉ

Les principes de sécurité s'articulent autour des responsabilités particulières en cette matière. Ces principes reposent sur une approche globale et une compréhension de la notion de sécurité des actifs informationnels de la part des utilisateurs. Des mesures de contrôle, de protection et de prévention sont appliquées.

Tel que spécifié à l'article 3.1 de la *Politique*, le CHUQ fait signer un engagement de confidentialité à tout utilisateur, et ce, par l'intermédiaire de l'officier de sécurité informationnelle, de la Direction des ressources humaines et du développement des compétences lors de l'embauche, de ses gestionnaires ou, s'il y a lieu, de toute autre personne désignée. Les contrats de service et ententes devront préciser les exigences en matière de sécurité.

### 7.2. RESPONSABILITÉ DE LA SÉCURITÉ

La Direction générale nomme une personne responsable de l'application de la *Politique*. Cette personne agit à titre d'officier de sécurité informationnelle du CHUQ.

### 7.3. ACCÈS AUX RENSEIGNEMENTS PERSONNELS

Le CHUQ limite l'accès aux renseignements personnels. Ces renseignements ne sont accessibles que s'ils sont absolument indispensables à l'exercice des fonctions de chaque utilisateur.

Les privilèges d'accès sont attribués par les personnes autorisées et sont consignés dans un registre supervisé par l'officier de sécurité informationnelle, mais tenu à jour par les responsables des accès.

Toute personne qui reçoit un privilège d'accès s'engage à ne pas divulguer, sauf dans le cadre de son travail, les renseignements personnels dont elle a pu prendre connaissance. Notamment, il est interdit de consulter, de divulguer ou d'imprimer des résultats d'examen, que ce soit pour soi-même, l'un de ses proches ou toute autre personne, si ce résultat est non relié aux besoins de sa fonction. En cas de violation de cet engagement, le CHUQ pourra imposer des sanctions disciplinaires ou administratives.

L'officier de sécurité informationnelle ou toute autre personne autorisée peut réviser, suspendre ou révoquer un privilège d'accès lorsque, entre autres raisons, la personne :

- Quitte définitivement le CHUQ ou est congédiée;

<b>RENOI(S) :</b> Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)	Page 5 de 15  DIC : 1-2-1
---	---------------------------------

<b>OBJET :</b> POLITIQUE EN MATIÈRE DE SÉCURITÉ INFORMATIONNELLE	<b>POLITIQUE N° 02-7100</b>
---	-----------------------------

- Termine son contrat ou son assignation;
- Change de fonctions à l'intérieur du CHUQ et lorsque ses nouvelles fonctions n'exigent pas l'accès aux renseignements personnels;
- S'absente pour une période déterminée par le CHUQ ou pour une période prolongée de plus de 90 jours;
- N'a pas utilisé son code d'accès, après vérification préalable, depuis plus d'un an;
- Divulgue des renseignements personnels pour des raisons autres que celles prévues dans l'exercice de ses fonctions.

De plus, pour tout comportement déviant ou usage abusif des systèmes d'information qu'il constate, l'officier de sécurité informationnelle peut, entre autres, demander la révision, la suspension ou la révocation des privilèges d'accès.

#### 7.4. UTILISATION D'INTERNET, DE L'INTRANET ET DES RÉSEAUX D'INFORMATION DU CHUQ

Un utilisateur conserve le droit au respect de sa vie privée et de sa dignité lorsqu'il est au travail. Toutefois, cette protection n'est pas complète. En effet, l'employeur a le droit de gérer et protéger son « institution » et d'obtenir jusqu'à un certain point des renseignements sur ses utilisateurs, et ce, à plus forte raison lorsqu'il en est avisé au préalable.

Ce faisant, le CHUQ informe ses utilisateurs que l'utilisation d'Internet, du courrier électronique, de l'intranet et des réseaux d'information du CHUQ est mise à leur disposition aux fins de leur travail et non à des fins personnelles.

À cet égard, le CHUQ informe également ses utilisateurs qu'il a l'intention de surveiller lesdites utilisations et que, ce faisant, ils ne peuvent s'attendre à ce que ces utilisations aient un caractère privé ou confidentiel. Les actifs informationnels et de télécommunication, les outils Internet ou tout autre outil de travail qui est accessible par les réseaux d'information du CHUQ ne doivent pas être en violation des lois et règlements en vigueur. Ces outils utilisés pour des activités illégales entraînent des mesures disciplinaires ou administratives pouvant aller jusqu'au congédiement. De plus, le CHUQ s'engage à coopérer face à toute requête provenant des forces de l'ordre ou à la demande de tout autre organisme mandaté à cet effet.

Aucun utilisateur des réseaux d'information du CHUQ ne peut se servir d'un modem sur un poste de travail sans l'approbation de l'officier de sécurité informationnelle.

Il est interdit aux utilisateurs ou aux tiers de modifier les systèmes d'information ni d'installer un actif informationnel sans autorisation préalable des personnes responsables désignées. Par exemple, l'installation et, par conséquent, l'utilisation de jeux sur les systèmes d'information ne sont pas autorisées.

Sauf stipulation contraire, conformément à la [Loi sur le droit d'auteur](#) et notamment eu égard à l'application des règlements sur la propriété intellectuelle applicables à l'Université Laval, le CHUQ est le premier titulaire des droits d'auteur de toute œuvre portée sur ses systèmes d'information, incluant tout programme d'ordinateur, tout matériel transmis à des clavardages en ligne (« chat »), des forums

<b>RENOI(S) :</b> Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)	Page 6 de 15  DIC : 1-2-1
---	---------------------------------

**OBJET :** POLITIQUE EN MATIÈRE DE SÉCURITÉ  
INFORMATIONNELLE

**POLITIQUE N° 02-7100**

de discussion (« *newsgroups* »), des réseaux sociaux (« *Facebook* ») ou des pages *World Wide Web* (« *www* ») créées par un utilisateur, dans le cadre de son travail. Toute œuvre réalisée pour le CHUQ, mais dont l'auteur ne fait pas partie de son personnel, doit faire l'objet d'une cession conformément à la *Loi sur le droit d'auteur*.

Tout logiciel ou document téléchargé via Internet ou le RITM vers les réseaux d'information du CHUQ deviennent la propriété de celui-ci. Ils doivent être utilisés en accord avec leurs licences et leurs droits d'auteur. De plus, aucun utilisateur ne peut se servir des outils d'accès à Internet pour télécharger ou distribuer des données ou des logiciels piratés.

Tout document téléchargé doit être vérifié pour la présence de virus avant son exécution, sa lecture, son transfert, sa copie ou toute autre manipulation nécessitant son enregistrement sur quelque support des réseaux d'information du CHUQ. L'utilisateur est responsable du contenu desdits documents en ce qui a trait aux virus qui pourraient s'y trouver. En conséquence, le CHUQ exige l'emploi de logiciels antivirus à jour sur les ordinateurs entrant en communication avec tous les réseaux d'information et l'installation des mises à jour des systèmes d'exploitation (rustines, « *patches* ») lorsque rendues disponibles par les fabricants.

Les utilisateurs doivent respecter la confidentialité des connaissances, partielles ou totales, de la structure des réseaux d'information du CHUQ et ne peuvent divulguer, en tout ou en partie, cette information. De plus, les utilisateurs doivent s'assurer que leur utilisation des réseaux d'information n'altère pas la structure de ceux-ci.

## 7.5. ACCÈS AUX ACTIFS INFORMATIONNELS ET DE TÉLÉCOMMUNICATION

L'accès aux actifs informationnels et de télécommunication du CHUQ doit être contrôlé. Chaque système prévoit des privilèges d'accès différents selon les catégories de l'utilisateur concerné.

Le CHUQ limite l'accès à ses actifs informationnels et de télécommunication aux seuls utilisateurs dont les tâches l'exigent dans l'exercice normal de leurs fonctions et qui détiennent en conséquence un privilège d'accès approprié. Pour gérer les accès, la Direction des technologies de l'information s'est dotée d'un registre de délégations d'accès.

## 7.6. UTILISATION DU COURRIER ÉLECTRONIQUE

Tout utilisateur qui désire préserver le caractère confidentiel ou privé du contenu des courriers électroniques qu'il transmet doit utiliser des programmes ou autres techniques de cryptage ou d'encodage mis à sa disposition sur le poste dont il se sert pour transmettre son courrier électronique. Par ailleurs, il doit également être conscient que les courriers électroniques qu'il envoie peuvent, à son insu, être redirigés, imprimés, sauvegardés ou affichés sur des médias ou des systèmes d'information de tiers.

Le gestionnaire de système qui agit à titre d'administrateur d'un système de courrier électronique doit fixer des règles concernant les délais de conservation des messages en vigueur au CHUQ. Les copies des messages, notamment celles que peut garder en mémoire le fournisseur de services Internet, sont soumises aux mêmes dispositions. Dans les organismes publics, les règles de conservation des

### RENOI(S) :

Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2)  
Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)

<b>OBJET :</b> POLITIQUE EN MATIÈRE DE SÉCURITÉ INFORMATIONNELLE	<b>POLITIQUE N° 02-7100</b>
---	-----------------------------

documents sont inscrites dans un calendrier de conservation des documents produits par l'organisme et approuvé par Bibliothèque et Archives nationales du Québec.

Le CHUQ attribue un privilège d'accès aux boîtes de courrier à l'administrateur et à l'officier de sécurité informationnelle. Ces droits sont effectifs, pour l'administrateur, seulement pour la réexpédition de messages qui ne sont pas arrivés à destination. L'officier de sécurité informationnelle, ou une personne qu'il délègue, peut faire la surveillance du contenu des messages et la détection de fraude pour fins d'enquête ou sur mandat des autorités.

À propos de l'utilisation du courrier électronique en milieu de travail, le CHUQ s'accorde un droit de surveillance du trafic des boîtes de courrier. L'utilisation du courrier électronique fait l'objet de règles strictes, dont notamment les règles suivantes :

- L'usage du courrier électronique doit être limité aux messages et aux fichiers qui sont en lien avec le travail;
- L'usage du courrier électronique est interdit pour des fins syndicales;
- L'usage du courrier électronique pour des fins commerciales, non autorisées ou illégales, est interdit;
- La modification d'un message avant sa retransmission à un autre destinataire est interdite.

Comme précaution supplémentaire pour assurer la confidentialité des messages et des fichiers expédiés par courrier électronique, l'encodage ou le cryptage est recommandé. S'il s'agit d'une méthode de cryptage autre que le chiffrement mis à la disposition de l'utilisateur, l'utilisation d'un outil spécialisé autre devra être autorisée, au préalable, par l'officier de sécurité informationnelle.

S'il ne peut assurer le cryptage ou l'encodage d'un document à caractère confidentiel, l'utilisateur devra employer un autre moyen de communication pour acheminer ledit document ou obtenir l'autorisation de son supérieur immédiat avant de le transmettre sans chiffrement.

## 7.7. UTILISATION DU TÉLÉTRAVAIL

Seules les personnes expressément autorisées, au préalable, par leur supérieur immédiat à utiliser le télétravail ont accès aux services ou aux logiciels qui leur seront explicitement autorisés par l'officier de sécurité informationnelle selon des modalités précises.

Le contrôle de l'utilisation du télétravail est fait par l'officier de sécurité informationnelle, ou une personne qu'il délègue, selon les exigences du RITM.

## 7.8. UTILISATION D'UN ORDINATEUR PORTABLE

Les règles d'utilisation d'un ordinateur portable font partie intégrante de la [Politique concernant la sécurité des ordinateurs portables au CHUQ, n° 02-7100\(PORT\)](#), approuvée par le comité de direction le 15 septembre 2010.

<b>RENOI(S) :</b> Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)		Page 8 de 15  DIC : 1-2-1
---	--	---------------------------------

<b>OBJET :</b> POLITIQUE EN MATIÈRE DE SÉCURITÉ INFORMATIONNELLE	<b>POLITIQUE N° 02-7100</b>
---	-----------------------------

## 7.9. COPIES DE SÉCURITÉ

Des règles et des procédures concernant la prise des copies de sécurité, leur conservation, leur récupération et leur destruction sont établies par l'officier de sécurité informationnelle. Toutes les copies de sécurité doivent être entreposées dans un endroit sécuritaire, selon le calendrier de conservation des documents du CHUQ.

## 7.10. DÉVELOPPEMENT ET CONCEPTION D'APPLICATIONS ET PROJETS D'INFORMATISATION

Tout projet de développement et de conception d'applications, de même que tout projet d'informatisation ou de mise en œuvre, doivent tenir compte des obligations réglementaires et normatives en matière de sécurité des actifs informationnels.

## 7.11. UTILISATION DES IMPRIMANTES ET DES TÉLÉCOPIEURS

Toute personne qui achemine ou imprime un document contenant des renseignements à caractère confidentiel doit en assurer la confidentialité.

Les imprimantes et les télécopieurs doivent être placés de façon à éviter toute utilisation et observation non autorisées, donc dans un endroit surveillé et non accessible au public. Un périphérique doit être utilisé par les personnes autorisées par le détenteur de l'actif informationnel, selon les privilèges d'accès consentis à l'utilisateur. Les documents doivent faire l'objet d'une surveillance et être rangés dans un endroit sûr et non accessible facilement au public.

L'utilisateur du télécopieur doit en tout temps :

- Vérifier, avant la transmission d'un document, si les renseignements personnels qu'il contient peuvent en être extraits;
- Remplir un formulaire d'accompagnement (bordereau de transmission par télécopie) indiquant les renseignements suivants : nom, adresse, société ou firme, numéro de téléphone et de télécopieur du destinataire, identification de l'expéditeur ainsi que ses numéros de téléphone et de télécopieur;
- Vérifier si le numéro de téléphone composé dans la fenêtre du télécopieur correspond exactement au numéro du destinataire et annuler l'envoi en cas d'erreur;
- Vérifier le rapport de transmission ou de tentative de transmission non réussie à la fin de la communication;
- Vérifier auprès du destinataire si les documents transmis ont bien été reçus.

De plus, s'il s'agit de la transmission de renseignements personnels, l'utilisateur doit, en plus de ce qui précède :

- Vérifier le degré d'urgence de communiquer des renseignements personnels;
- Indiquer visiblement le caractère confidentiel;
- Aviser le destinataire de l'heure de la transmission et s'assurer de sa présence, ou de la présence d'une personne déléguée, au moment de la réception;

<b>RENOI(S) :</b> Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)		Page 9 de 15  DIC : 1-2-1
---	--	---------------------------------

<b>OBJET :</b> POLITIQUE EN MATIÈRE DE SÉCURITÉ INFORMATIONNELLE	<b>POLITIQUE N° 02-7100</b>
---	-----------------------------

- Obtenir la confirmation de la réception de l'envoi par la personne autorisée à recevoir la communication.

Pour ces envois spécifiques, le rapport de transmission peut être conservé par l'expéditeur.

Pour tous les documents imprimés ou reçus par télécopieur :

- L'utilisateur doit les récupérer rapidement et les remettre au destinataire;
- Les documents imprimés ou reçus par mégarde, qui ne sont pas destinés à l'utilisateur, doivent être détruits immédiatement et l'expéditeur doit en être avisé.

Pour toute autre information, nous nous référons à la [Politique et procédures de confidentialité et de gestion des dossiers des usagers, n° 10-2200](#).

## 8. RESPONSABILITÉS D'APPLICATION

Cette section vise à établir les rôles et responsabilités de chaque personne, selon les fonctions qu'elle occupe au sein du CHUQ, en ce qui a trait à la *Politique*.

### 8.1. LE CONSEIL D'ADMINISTRATION

- Adopte la *Politique*, de même que ses mises à jour.

### 8.2. LA DIRECTION GÉNÉRALE

- Assure l'application de la *Politique* dans l'organisation;
- Adopte le bilan annuel concernant la sécurité des actifs et le transmet au coordonnateur de la sécurité des actifs informationnels au niveau régional;
- Apporte les appuis financiers et logistiques nécessaires à la mise en œuvre et à l'application de la *Politique*;
- Informe et mobilise les gestionnaires et le personnel sur l'application de la *Politique*;
- Nomme l'officier de sécurité informationnelle qui agit à titre de responsable de la sécurité des actifs informationnels du CHUQ ainsi que les assistants de la sécurité, leur fait connaître leurs responsabilités et leur délègue les pouvoirs requis pour appliquer la *Politique*.

### 8.3. L'OFFICIER DE SÉCURITÉ INFORMATIONNELLE

En collaboration avec les gestionnaires, et plus particulièrement avec la Direction des technologies de l'information dans le cadre de l'exercice de son mandat, assume les responsabilités suivantes :

- Élabore et met à jour la *Politique*, la soumet à la Direction générale et au conseil d'administration pour adoption;
- Préside le comité de sécurité informationnelle ou y délègue une personne;

<b>RENOI(S) :</b> Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)	Page 10 de 15  DIC : 1-2-1
---	----------------------------------

<b>OBJET :</b> POLITIQUE EN MATIÈRE DE SÉCURITÉ INFORMATIONNELLE	<b>POLITIQUE N° 02-7100</b>
---	-----------------------------

- Établit un programme général d'application et de respect de la *Politique* conformément aux orientations régionales;
- Fait connaître l'importance de l'application de la *Politique* et identifie avec les gestionnaires les détenteurs d'actifs informationnels;
- Met en œuvre, participe et élabore un programme général d'information, de sensibilisation et de formation à l'intention du personnel et des tiers, le cas échéant;
- Gère les aspects relatifs aux incidents impliquant un manquement à la sécurité des actifs informationnels et de télécommunication et procède à des évaluations de la situation en matière de sécurité;
- S'assure que toutes les directions du CHUQ acquièrent les équipements et le matériel nécessaires à l'application de la *Politique*, identifie les problèmes pouvant se présenter, propose des solutions s'il y a lieu et coordonne la mise en place de ces solutions;
- Produit un bilan annuel relatif à l'application de la *Politique*; par la suite, met en œuvre les actions pour apporter les correctifs qui s'imposent suite aux lacunes identifiées lors de la parution du bilan annuel;
- Prévoit annuellement et au besoin les bilans et rapports relatifs à la sécurité des actifs informationnels du CHUQ en s'assurant que l'information sensible à diffusion restreinte est traitée de manière confidentielle; après approbation, les soumet au coordonnateur régional de la sécurité des actifs informationnels de la région de Québec;
- Coordonne, avec le responsable de l'accès à l'information, toutes les activités reliées à la protection des renseignements personnels;
- Coordonne la sécurité concernant les actifs informationnels et de télécommunication;
- Autorise l'utilisation de certains équipements spécialisés selon les normes de sécurité reconnues, en tenant compte de la mission et des mandats du CHUQ;
- Vérifie périodiquement que le programme général de sécurité concernant les actifs informationnels, de télécommunication et de protection des renseignements personnels est respecté et suit la mise en œuvre de toute recommandation découlant d'une vérification ou d'un audit;
- Élabore des ententes avec les fournisseurs de services, ou entre les établissements ou les organismes, afin de respecter les lois et les règlements en vigueur au Québec concernant la confidentialité des données confidentielles ou sociosanitaires nominatives et l'utilisation des technologies de l'information.

#### 8.4. LE SUPÉRIEUR IMMÉDIAT DE L'UTILISATEUR

- Applique la *Politique* à l'intérieur de la direction ou du secteur d'activité dont il a la gestion;
- S'assure que les mesures de sécurité appropriées sont élaborées, approuvées, mises en place et appliquées systématiquement dans son secteur d'activité;
- Applique les sanctions prévues à la *Politique* lors d'un manquement à la sécurité de la part d'un membre du personnel faisant partie de sa direction ou de son secteur d'activité;

<b>RENOI(S) :</b> Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)	Page 11 de 15  DIC : 1-2-1
---	----------------------------------

<b>OBJET :</b> POLITIQUE EN MATIÈRE DE SÉCURITÉ INFORMATIONNELLE	<b>POLITIQUE N° 02-7100</b>
---	-----------------------------

- S'implique dans l'ensemble des activités relatives à la sécurité;
- Détermine les règles d'accès aux actifs sous sa responsabilité avec l'appui de l'officier de sécurité informationnelle.

## 8.5. LES UTILISATEURS

- Signent un engagement de confidentialité avec le CHUQ;
- Respectent la *Politique* et les procédures qui en découlent;
- Font part de toute situation problématique susceptible de compromettre la sécurité des actifs informationnels du CHUQ;
- Sont imputables de leur manquement à la *Politique*.

## 9. AUTRES DISPOSITIONS

### 9.1. PROGRAMME D'INFORMATION, DE SENSIBILISATION ET DE FORMATION DU PERSONNEL

Le CHUQ met en œuvre un programme d'information, de sensibilisation et de formation du personnel dans le but de l'informer de ses responsabilités et de la nécessité de protéger l'accès aux données sociosanitaires confidentielles, et aussi dans le but d'assurer la sécurité concernant l'utilisation des actifs informationnels et de télécommunication.

### 9.2. MANQUEMENT À LA SÉCURITÉ

L'officier de sécurité informationnelle doit faire enquête sur tout manquement à la sécurité informationnelle et appliquer les mesures correctrices qui s'imposent au niveau informatique. Il doit aussi faire un rapport, selon des modalités prédéterminées et approuvées par le CHUQ, au supérieur immédiat de l'utilisateur et à la Direction des ressources humaines et du développement des compétences qui prendront les mesures administratives ou disciplinaires pour toute contravention à la *Politique* ou pour toute mauvaise utilisation des réseaux d'information du CHUQ.

Tout membre du personnel qui contrevient à la [Procédure concernant les règles d'utilisation des systèmes d'information du CHUQ, n° 02-7100-01](#), découlant de la présente *Politique*, est notamment passible des sanctions suivantes :

- Mesures administratives et disciplinaires ou autres sanctions appropriées à l'intention du personnel conformément aux lois, règlements et conventions collectives de travail en vigueur;
- Révocation de certains privilèges d'accès aux équipements et services visés par la *Politique*;
- Remboursement au CHUQ de toute somme, y compris les sommes émanant d'un jugement prononcé par tout tribunal ou organisme réglementaire quelconque à l'endroit du CHUQ et qui découlerait de l'utilisation non autorisée, frauduleuse ou illicite de ses services ou de ses actifs informationnels et de télécommunication ou de ses systèmes d'information.

<b>RENOI(S) :</b> Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)	Page 12 de 15  DIC : 1-2-1
---	----------------------------------

**OBJET :** POLITIQUE EN MATIÈRE DE SÉCURITÉ  
INFORMATIONNELLE

**POLITIQUE N° 02-7100**

De plus, le requérant s'engage à rembourser les frais de réparation ou autres frais encourus par le CHUQ et qui seraient reliés à une utilisation non autorisée, inadéquate ou malveillante dudit équipement, selon le tarif horaire applicable.

## 10. PROCÉDURE DÉCOULANT DE LA POLITIQUE

La procédure suivante découle de la présente *Politique* :

- [Procédure concernant les règles d'utilisation des systèmes d'information du CHUQ, n° 02-7100-01.](#)

## 11. RÉFÉRENCES

Les documents ayant servi de référence pour l'élaboration de la *Politique en matière de sécurité informationnelle* sont les suivants :

CANADA. *Code criminel*, L.R.C., 1985, c. C-46.

CANADA. *Loi sur le droit d'auteur*, L.R., 1985, c. C-42.

MINISTÈRE DE LA SANTÉ ET DES SERVICES SOCIAUX. *Cadre global de gestion des actifs informationnels appartenant aux organismes du réseau de la santé et des services sociaux – Volet sur la sécurité*, Québec, MSSS, 2002, 76 p.

QUÉBEC. *Charte des droits et libertés de la personne*, L.R.Q., c. C-12.

QUÉBEC. *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1.

QUÉBEC. *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1.

QUÉBEC. *Loi sur les services de santé et les services sociaux*, L.R.Q., c. A-4.2.

## 12. MÉCANISMES DE RÉVISION

La présente *Politique* sera mise à jour à la suite de modifications apportées au cadre légal ainsi qu'aux lois et règlements en vigueur, ou bien pour tenir compte des nouvelles pratiques et technologies utilisées au CHUQ ainsi que des besoins exprimés, le cas échéant. Sinon elle sera révisée au plus tard le 27 septembre 2013.

Toute modification apportée à la présente *Politique* doit être approuvée par le conseil d'administration du CHUQ.

### RENVOI(S) :

Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2)  
Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)

<b>OBJET :</b> POLITIQUE EN MATIÈRE DE SÉCURITÉ INFORMATIONNELLE	<b>POLITIQUE N° 02-7100</b>
---	-----------------------------

### 13. APPROBATION ET ENTRÉE EN VIGUEUR

La présente politique remplace celles adoptées par le conseil d'administration en 2000 et en 2004 et ayant les même objets.

La présente *Politique en matière de sécurité informationnelle* entre en vigueur le jour de son adoption par le conseil d'administration du CHUQ, soit le 27 septembre 2010.

**CENTRE HOSPITALIER UNIVERSITAIRE DE QUÉBEC**

Direction des technologies de l'information

(2010-09-27)

YF/md

P:\DPE\PERFORMANCE\02- GESTION DOCUMENTAIRE\_02-1500\01 - GESTION ORG ADM\01-4100 - POL PRO REG adm CHUQ\RECUEIL pol-pro-reg du CHUQ\1\_POL-PRO\02 - RESS INFORM\02-7100\_POL\_Sécurité\_informtionnelle-RECUEIL.doc

<p><b>RENOI(S) :</b> Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1)</p>	<p>Page 14 de 15</p> <p>DIC : 1-2-1</p>
--	---

**OBJET :** POLITIQUE EN MATIÈRE DE SÉCURITÉ  
INFORMATIONNELLE

**POLITIQUE N° 02-7100**

## ANNEXE

- **ANNEXE 1 — Engagement de confidentialité type**

**RENOI(S) :**

Loi sur les services de santé et les services sociaux (L.R.Q., c. S-4.2)  
Loi sur l'accès aux documents des organismes publics et sur la  
protection des renseignements personnels (L.R.Q., c. A-2.1)

## ENGAGEMENT DE CONFIDENTIALITÉ TYPE

Par la présente, je (*nom*) \_\_\_\_\_ (*prénom*) \_\_\_\_\_, (*fonction ou titre d'emploi*) \_\_\_\_\_ au Centre hospitalier universitaire de Québec (CHUQ) dont le siège social est situé au 11, côte du Palais à Québec, confirme avoir été informé de l'existence de la *Politique en matière de sécurité informationnelle du CHUQ* dont le texte intégral est disponible sur demande en format papier à la DRHDC, auprès de mon chef de service, sur le réseau Internet ([www.chuq.qc.ca/politiques](http://www.chuq.qc.ca/politiques)) et sur l'intranet du CHUQ sous l'onglet « Politiques, procédures et règlements du CHUQ ».

Je m'engage à prendre connaissance de cette *Politique* ainsi que des codes de conduite applicables, à y adhérer et à les respecter. Je dois en tout temps prendre toutes les mesures mises à ma disposition, afin d'appliquer cette politique dans l'exercice de mes fonctions et des tâches qui y sont associées.

J'ai le devoir d'informer immédiatement mon supérieur immédiat de tout incident ou toute situation portée à ma connaissance qui serait susceptible de compromettre la confidentialité des renseignements confidentiels et la sécurité concernant l'utilisation des actifs informationnels et de télécommunication.

Je m'engage à ne jamais dévoiler des renseignements susceptibles de mettre en péril soit la confidentialité des renseignements et des données sociosanitaires confidentielles auxquels j'ai accès, soit la sécurité des actifs informationnels et de télécommunication du CHUQ.

Je suis pleinement conscient que le CHUQ utilise des logiciels de sécurité qui peuvent enregistrer, pour des fins de gestion, le contenu de mon courrier électronique, les adresses Internet des sites que je visite et conserver un dossier de toute activité réalisée sur ses réseaux d'information au cours de laquelle je transmets ou reçois quelque document que ce soit lorsque j'utilise les systèmes d'information et les ressources du CHUQ.

J'ai été informé que le CHUQ peut enregistrer et archiver, pour des fins de gestion, les messages que je reçois ou envoie et peut me soumettre, de manière ponctuelle, à un audit ou à une vérification informatique, si requis par l'officier de sécurité informationnelle du CHUQ. J'ai été informé également qu'il pourrait y avoir des mesures administratives ou disciplinaires prises à mon égard dans le cas où je manquerais à mes engagements.

Je conserve le droit au respect de ma vie privée et de ma dignité lorsque je suis au travail. Toutefois, cette protection n'est pas complète. En effet, l'employeur a le droit de gérer et protéger son « institution » et d'obtenir jusqu'à un certain point des renseignements sur ses utilisateurs, et ce, à plus forte raison lorsqu'il en est avisé au préalable.

Je suis informé qu'Internet, le courrier électronique, l'intranet et les réseaux d'information du CHUQ sont mis à ma disposition aux fins de mon travail et non à des fins personnelles.

Je suis informé également que le CHUQ a l'intention de surveiller lesdites utilisations et que, ce faisant, il ne peut s'attendre à ce que ces utilisations aient un caractère privé ou confidentiel. Les actifs informationnels et de télécommunication, les outils Internet ou tout autre outil de travail qui est accessible par les réseaux d'information du CHUQ ne doivent pas être en violation des lois et règlements en vigueur. Ces outils utilisés pour des activités illégales entraînent des mesures disciplinaires ou administratives pouvant aller jusqu'au congédiement. De plus, le CHUQ s'engage à coopérer face à toute requête provenant des forces de l'ordre ou à la demande de tout autre organisme mandaté à cet effet.

\_\_\_\_\_  
**Signature de l'utilisateur**

Prénom et nom

**Numéro d'employé du CHUQ :** \_\_\_\_\_

\_\_\_\_\_  
**Date**

\_\_\_\_\_  
**Signature du représentant du CHUQ**

Prénom et nom

\_\_\_\_\_  
**Date**

*Original au dossier.*